The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:

02/20/2014

SUBJECT:

Multiple Vulnerabilities in Adobe Flash Player Could Allow Remote Code Execution (APSB14-07)

EXECUTIVE SUMMARY:

Multiple vulnerabilities have been discovered in Adobe Flash Player that could allow an attacker to remotely take control of the affected system. Adobe Flash Player is a multimedia platform used to add animation and interactivity to web pages. Successful exploitation could result in an attacker gaining the same privileges as the logged on user. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts will likely cause denial-of-service conditions.

THREAT INTELLIGENCE:

At this time, these vulnerabilities are not publicly disclosed and there is no known proof-of-concept code available.

SYSTEMS AFFECTED:

- Adobe Flash 12.0.0.44 and earlier for Windows and Mac
- Adobe Flash 11.2.202.336 and earlier for Linux

RISK:

Government:

- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:

- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

TECHNICAL SUMMARY:

Adobe has released a security update for Adobe Flash Player 12.0.7.148 and earlier versions on the Windows and Macintosh operating systems and version 11.2.202.336 for Linux systems. This update addresses critical vulnerabilities that could potentially allow an attacker to remotely take control of the affected system. Adobe recommends updating their respective clients to the most recent version available.

RECOMMENDATIONS:

The following actions should be taken:

- Install the updates provided by Adobe immediately after appropriate testing.
- Remind users not to visit untrusted websites or follow links provided by unknown or untrusted sources.
- Do not open email attachments from unknown or untrusted sources.

REFERENCES:

Adobe:

http://helpx.adobe.com/security/products/flash-player/apsb14-07.html

CVE:

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0502

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0499

http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2014-0498